Prepared Testimony and Statement for the Record of Ben Buchanan

Postdoctoral Fellow, Belfer Center Cybersecurity Project Harvard University

My name is Ben Buchanan. I'm a fellow at Harvard University's Belfer Center for Science and International Affairs and a Global Fellow at the Woodrow Wilson International Center for Scholars. The primary focus of my research is examining how nations use their capabilities for attack and espionage in cyberspace against one another, and examining the strategies that drive this usage.

One nation of great interest in this research is the Russian Federation. Over the past few years, I have spent much time trying to understand Russian cyber operations, how investigators can attribute particular activities to Russia or other states, how electoral processes can be interfered with, and what broader strategic dynamics are at play. In light of this work, I'd like to make three points to begin our discussion.

First, we often think of Russian hacking as something that is new and different, but to do so is to be ignorant of history. There is a demonstrated pattern of Russian cyber operations stretching back several decades. One major early case, dating from the late 1990s, is commonly referred to as Moonlight Maze. In that case, Russian hackers penetrated a wide range of American networks for espionage purposes. Since then, Russian cyber operations have continued to expand greatly, hacking into key military, political, and economic institutions.

These operations show adeptness in several ways. Perhaps most significant is that they demonstrate how the Russians have developed new digital methods to accomplish old tasks. A series of espionage cases show the Russian aptitude for gathering information using computer hacking. The 2007 attacks on Estonia and Georgia are an exhibit of how Russia uses cyber operations against democratic states. Though we have somewhat less information about it, the 2015 blackout in Ukraine—the first ever publicly known case of a power outage caused by cyber attack—shows the potency of cyber attacks that appear to be Russian in origin. And the 2016 election interference demonstrates that the Russians have married their longstanding history of influence operations with their more recently developed capacity for hacking.

While Russia is not the only nation to employ cyber operations to advance its own interests, the ways in which it has done so—and the threat its activities pose to democracies and to their fundamental institutions—deserve great scrutiny and, often, resistance.

Second, there is a damaging perception that it is impossible to understand who is responsible for which activities in cyberspace. This is sometimes called the attribution problem, and it is not nearly the impassable roadblock that it is sometimes made out to be. Alongside Professor Thomas Rid of King's College London, I spent a year investigating how it is possible to do attribution in cyberspace. After technical study and interviews with computer forensics experts in the private sector and in multiple intelligence agencies, we concluded that not only is accurate attribution possible, but that

advanced nations such as the United States do it regularly. It is possible to do some form of attribution by relying on forensics data—such as language, infrastructure, exploit, and time zone indicators, among many others. For intelligence agencies, human and signals intelligence sources can provide additional vital information on the intentions of another nation, and can confirm attribution hypotheses.

Rarely is any single piece of evidence by itself conclusive when it comes to doing attribution. Hackers do, sometimes, leave false flags to try to mislead investigators. Nonetheless, the United States intelligence community and private sector firms have overcome the attribution problem in many instances in recent years, and have developed a strong understanding of how various nations, including Russia, operate in cyberspace.

As early as the middle of last summer, the technical evidence strongly indicated that the Russians were responsible for the hacking activities against the Democratic National Committee and other related entities. The United States intelligence community report gives me still greater confidence in this assessment. In short, when it comes to many major Russian activities, attribution is simply not an issue.

Third, I'd like to close by taking a broader view. Every cyber activity takes place in a strategic context, and we would do well to remember that context when we analyze operations and consider responses. Old strategic ideas, such as deterrence, do not go away when it comes to this new mode of engagement between nations, though they are often difficult at first to translate.

Many of the Russian activities occur, I believe, because Russia has developed the capability to act, senses an opportunity to do so, and calculates that the benefits of the operations will exceed the costs.

In short, we have not yet been able to devise means of deterrence in cyberspace that extend to the kinds of activities we are discussing today. Establishing deterrence with our own cyber capabilities has proven challenging, in part because we have not always communicated our resolve well, and in part because we are rightly worried about further escalation.

These difficulties are important and deserve strategic attention. We must find ways to better defend our vital computer systems, denying adversaries the opportunity to act. We must develop methods of deterrence that impose costs for significant malicious actions, and we must communicate those clearly.

I am mindful of the lesson from history—sometimes called the security dilemma—that nations often unintentionally threaten one another as they protect their own interests. I have written a great deal about how the cybersecurity dilemma can arise. And so I believe we must develop a strategy that protects our interests but does not unduly threaten other nations. Calibrating a response in this fashion is not an easy task, but it is a vital one.

After what has happened this past year, few issues are more important right now. Thank you.